FORT KNOX ACCEPTABLE USE POLICY (AUP)

For use of this form, see AR 25-2

1. Scope. This policy applies to all soldiers, civilians, and contractors who plan, deploy, configure, operate, and maintain data communication resources that are attached either directly or indirectly to the Fort Knox Campus Area Network (CAN). The scope of this document includes the Fort Knox CAN, computers, Portable Electronic Devices (PED), and services. All networks within the Fort Knox installation boundaries are considered Fort Knox Information Systems (IS) networks.

2. Understanding. I understand that my responsibility is to safeguard all information that is accessed by me from any unauthorized or inadvertent modification, disclosure, destruction, denial of service, or use.

3. Access. Access to the Fort Knox CAN is for official, authorized use as set forth in DoD 5500.7-R, "Standards of Conduct;" AR 25-2; and any further limitations this policy may establish.

4. Revocability. Access to Fort Knox resources is a revocable privilege and is subject to monitoring and security scans for Information Assurance Vulnerability Alert (IAVA) compliance.

5. Minimum Security Rules and Requirements. As a Fort Knox IS user, the following minimum security rules and requirements apply:

a. I will not be permitted access to any network unless I am in complete compliance with personnel security standards outlined in AR 25-2.

b. I have read the Fort Knox Computer User Guide, completed the user security awareness training provided at http://ia.gordon.army.mil, and the Certification of Completion has been provided to my Information Assurance Security Officer (IASO).

c. I am responsible for all activities that occur under my individual account or CAC login once my password/PIN has been issued to me. I will generate, store, and protect passwords/PINs IAW AR 25-2.

d. I will only use authorized hardware and software. I will not install or use any personally owned hardware, software, shareware, or public domain software.

e. I will use virus-checking procedures before uploading or accessing information from any government system, diskette, attachment, compact disk, or USB drive.

f. I will use operating systems and programs only as specifically authorized, ensuring they are not altered, changed, or re-configured.

g. Computer equipment maintenance will only be performed by a Directorate of Information Management (DOIM) recognized/approved source.

h. While I am logged on, I will not leave my computer unattended. If I do leave my work area, I will secure my computer by removing my CAC card and engage the "lock computer" utility. I will leave my computer powered on 24 hours a day, as directed by DOIM. When leaving for the day, I will use the "log off" feature from the Start menu--not the "lock computer" utility.

i. I will immediately report any suspicious output, files, shortcuts, or system problems to the System Administrator (SA) and/or IASO/IMO.

j. I will use Government information systems (computers, systems, peripherals, and networks) only for authorized purposes. I understand that access to Army resources is a revocable privilege and is subject to monitoring and security testing.

k. I understand that monitoring will be conducted for security purposes and that any information captured during monitoring may be used for administrative/disciplinary actions or for criminal prosecution.

l. I will not connect wireless or Bluetooth devices to government equipment. Only exception is a wireless mouse.

m. I will ensure that only one connection to the Fort Knox CAN on a workstation is enabled at any given time--any combination of two or more simultaneous connections, i.e., direct connect, modem, or wireless is strictly prohibited.

n. I understand the Army's Data-At-Rest Best Business Practice and will ensure that any sensitive information (includes but not limited to FOUO, HIPPA, personally identifiable information) will be placed in an encrypted folder on a laptop or USB drive and also will encrypt the data when sending it through e-mail.

o. I will not use my government e-mail address on any private or public web site except when necessary to conduct business in an official government capacity.

p. I will ensure that any quotes that are part of my e-mail signature block are professional in nature.

6. Unacceptable Use. The following activities are strictly prohibited:

- Accessing pornography or obscene material (adult or child).
- Gambling.
- Transmitting chain letters. This includes warnings about the "latest virus" with instructions to forward to everyone you know.
- Advertising, soliciting, or selling for commercial or private gain.
- Using unauthorized peer-to-peer software (i.e., Gnutella, Napster, iTunes, Kazaa, Limeware, MP3 music and video files or games, etc.)
- Copyright infringement (i.e., unauthorized copying/distribution of software, music, books, photographs, etc.)
- Any unlawful conduct.
- Attaching any privately owned and/or unaccredited hardware to the NIPRNET. This includes laptops, peripheral devices, and USB storage devices.
- Personal use other than as authorized by both the DAA and my supervisor.
- Streaming data or tickers from the internet (automatic download programs that keep abreast of stock prices, sports scores, and news) (i.e., e-trade, ESPN, CNN, Weatherbug, live audio/video, etc.)
- Internet game play (i.e., Fantasy Football, Scrabble, Quake, etc.)
- Connecting employee-owned computers, electronic devices, or media to government network ports and/or equipment.
- Forwarding official email to non-official accounts or devices.
- Internet Chat or instant messenger services (i.e., AOL, MSN, Yahoo, etc.) except for AKO chat which is an Army chat forum.
- Introduction of executable or malicious code (i.e., .exe, .vbs, or .bat files, etc.) without prior authorization of the DOIM.
- Attempt to access or process data exceeding the authorized IS classification level.
- Using Government systems to bid on online auctions or receive personal payments, prizes, and giveaways.

7. Enforcement. Any personnel found violating this policy may be subject to disciplinary actions as outlined in the Uniform Code of Military Justice (UCMJ) or under other disciplinary administrative, or contractual actions as applicable. Personnel who fail to comply with these requirements and are not subject to UCMJ will be subject to disciplinary, administrative, or prosecutorial actions as authorized from criminal or civil sanctions under sections including, but not limited to, the United States Code, contractual support obligations, or Federal or state regulations.

8. Acknowledgement. I have read the above requirements regarding use/access to the Fort Knox CAN and the Computer User Guide. I understand my responsibilities regarding the protection and use of these systems and the information contained in them. I will safeguard and mark with the appropriate classification level all information created, copied, stored, or disseminated from the IS and will not disseminate it to anyone without a specific need to know.

9. Point of Contact. The POC for this policy is the Installation Information Assurance Manager, Directorate of Information Management.

NOTICE: Expires 1 year from date of signature. Annual authentication is required.

LAST NAME, FIRST NAME, MI:		RANK/GRADE:	PHONE NUMBER:
UNIT/DIRECTORATE/ACTIVITY:		AKO E-MAIL ADDRESS: @us.army.mil	
SIGNATURE:	DATE:	IASO'S SIGNATURE:	DATE: